whereby placement of the sensor site in the casing of the pen-based computing device enables a continuous capture of a facial image print while the pen-based computing device is being used.

REMARKS

Applicant acknowledges and thanks the Examiner for his careful and thorough examination of the present application. Favorable reconsideration is respectfully requested.

In the Office Action of February 24th, 2005, the Examiner objected to the drawings lacking reference numerals (except FIGURES 3A and 3B). Enclosed with this Amendatory Response are replacement sheets for FIGURE 1, FIGURES 1A and 1B, FIGURES 2A and 2B, and FIGURES 4A and 4B. The only changes made to these drawings are the addition of such reference numerals, which are circled. These drawing changes necessitated the addition of these reference numerals to the specification. These changes are also incorporated in this Amendatory Response. Also, three typographical errors, each being clear from a reading of the specification, are being amended; one on Page 6, Line 12 (adding the word "sensor"), another on Page 9, Line 6 (adding the word "sensor"), and another on Page 9, Line 8 (deleting the word "sensor"). No new matter has been added.

The Examiner rejected all pending claims (1-17) under 35 U.S.C. §112, second paragraph, because the use of the phrases "seamless" and "routine computer usage" made the claims indefinite. Rather than amending the existing claims to modify such language, Applicant has opted to cancel all pending claims and replace them with three new claims.

In the above-identified Office Action, the Examiner rejected Claims 1, 3-7, 9-14, 16, and 17 under 35 U.S.C. §102(a) as being anticipated by U.S. Patent 6,182,221 (Hsu et al.); and he rejected Claims 2, 8, and 15 under 35 U.S.C. §103(a) as being obvious by the combination of U.S. Patent 6,182,221 (Hsu et al.) and U.S. Patent 6,076,167 (Borza).

The test for determining if a reference anticipates a claim, for purposes of rejection

under 35 USC §102, is whether the reference discloses all of the elements of the claimed combination, or the mechanical equivalents, functioning in substantially the same way to produce substantially the same results. As noted by the Court of Appeals of the Federal Circuit in ***Lindemann Maschinenfabrik GmbH v. American Hoist and Derrick***, 221 USPQ 481, 485 (1984), in evaluating the sufficiency of an anticipation rejection under 35 USC §102, the Court stated:

> "Anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim."

Applicant has opted to focus attention herein to Claim 13. Rather than patch Claim 13 to eliminate the "seamless" and "routine computer usage" language objected to by the Examiner, Applicant has opted to rewrite it. Claims 18, 19, and 20 are essentially a rewrite of old Claim 13, their sum total being somewhat narrower in scope. Claim 13 included the word "biometric" to refer to the type of image captured. The new claims are more specific: Claim 18 is limited to the capture of a thumbprint image; Claim 19 is limited to the capture of palm print image; and Claim 20 is limited to the capture of a facial image. Also, the three claims are now directed to pen-based computers.

SUMMARY OF THE INVENTION

Applicant's invention, as now claimed, is quite specific, being directed to the capture of biometric data captured by a pen-based computer when access is requested through the pen-based computer to secure data, and the placement of the biometric sensor. In each instance, the placement of the thumbprint sensor (Claim 18), palm print sensor (Claim 19), or facial image sensor (Claim 20) enables a continuous capture of the biometric image. For example, Claim 18 now requires the placement of the fingerprint sensor site in the casing of the pen-based computing device enabling (1) capture of the thumbprint image (2) of the user hand holding the pen-based computing device (3) for purposes of identity authentication prior to each request to access the secure data while the pen-based computing device is held. The image capture is incidental in that it is unnecessary for the user even to know each time the image is captured.

Also, the claims are now directed to pen-based computers. With regard to Claims 18 and 19, while one hand of the user is using a stylus to scroll through screens, the hand of the user holding the pen-based computer is used to capture biometric data to confirm user identity. This feature also enables the biometric data to be captured and preserved as a time and date stamp for each such access request.

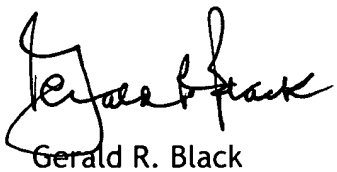
U.S. Patent 6,182,221 (Hsu et al.) involves remote cellular phone access by use of fingerprint sensors. But the reference is silent as to the issues of sensor placement and incidental capture. And, since each of the three pending claims of the present invention only recite the capture of one biometric, U.S. Patent 6,076,167 (Borza) is no longer an issue. Neither the Hsu reference nor the Borza reference teaches, discloses, or even suggests the issue of sensor placement or provides an incidental capture of biometric data. Clearly, Claims 18, 19, and 20, as amended, are patentable over either reference or their combination.

Conclusion

In view of the foregoing remarks, it is respectfully submitted that the present application is in condition for allowance. An early notice thereof is earnestly solicited. If after reviewing this Response, there are any remaining informalities which need to be resolved before the application can be passed to issue, the Examiner is invited and respectfully requested to contact the undersigned by telephone in order to resolve such informalities.

May 12, 2005

Respectfully submitted,



Gerald R. Black
Registration Number 29,514
30590 Southfield Road, Suite #160
Southfield, Michigan 48076
248.644.1014 phone
413.521.4703 fax

CLAIMS

(CLEAN COPY)

18 (New). A pen-based computing device for accessing secure data, the pen-based computing device having a casing, the pen-based computing device including at least one fingerprint sensor for capturing a user thumbprint image of a user hand, the fingerprint sensor being positioned at a fingerprint sensor site in the casing of the pen-based computing device;

whereby placement of the fingerprint sensor site in the casing of the pen-based computing device enables an incidental capture of the thumbprint image of the user hand for purposes of identity authentication prior to each request to access the secure data; and

whereby placement of the fingerprint sensing site in the casing of the pen-based computing device enables capture of the thumbprint image of the user hand holding the pen-based computing device; and

whereby placement of the fingerprint sensing site in the casing of the pen-based computing device enables a continuous capture of the thumbprint image of the user hand while the pen-based computing device is being held.

19 (New). A pen-based computing device for accessing secure data, the pen-based computing device having a casing, the pen-based computing device including a palm-print sensor for capturing a palm-print image of a user hand, the palm-print sensor being positioned at a palm-print sensor site in the casing of the pen-based computing device;

whereby placement of the palm-print sensor site in the casing of the pen-based computing device enables an incidental capture of the palm-print image of the user hand for purposes of identity authentication prior to each request to access the secure data; and

whereby placement of the palm-print sensing site in the casing of the pen-based computing device enables capture of the palm-print image of the user hand holding the computing device; and

whereby placement of the palm-print sensing site in the casing of the pen-based computing device enables a continuous capture of a palm-print image of the user hand while the pen-based computing device is being held.

20 (New). A pen-based computing device for accessing secure data, the computing device having a casing, the pen-based computing device including a palm-print sensor for capturing a facial image print, the facial image print sensor being positioned at a sensor site in the casing of the pen-based computing device;

whereby placement of the palm-print sensor site in the casing of the pen-based computing device enables an incidental capture of the facial image of a user for purposes of identity authentication prior to each request to access the secure data; and

whereby placement of the sensor site in the casing of the pen-based computing device enables a continuous capture of a facial image print while the pen-based computing device is being used.

BRIEF DESCRIPTION OF THE DRAWINGS

FIGURE 1 is a schematic the preferred embodiment of the network system of the present invention;

FIGURE 1A is a schematic the first preferred embodiment of the backside of a computing device of the present invention for use with the data security system of FIGURE 1, the computing device (30C) enabling biometric authentication prior to accessing network data, the computing device (30C) being handheld and portable, the handheld computer (30C) being pen-based, the handheld computer (30C) comprising a stylus (50) for operating such computing device (30C), the computer (30C) being remote from a host processor (12) and enabling access to network data, the computer (30C) including a pair of fingerprint sensors (15) embedded in the casing of the handheld computer (30C), one fingerprint sensor (15) capturing a print image of the user's thumb and the second fingerprint image sensor (15) capturing a print image of the user's index finger, both being of the user's left hand;

FIGURE 1B discloses the stylus of FIGURE 1A, the stylus including a fingerprint sensor in the stylus barrel for enabling capture of a fingerprint image when the stylus is grasped;

FIGURE 1C discloses the front-side of the handheld computer of FIGURE 1A, the handheld computer including a fingerprint sensor embedded into the casing of the handheld computer at a site such that the image of the thumb of the user is captured during usage of the handheld computer;

FIGURES 2A and 2B disclose a second preferred embodiment of the front-side and the backside respectively of the computing device of the present invention for use either with the data security system of FIGURE 1 or as a stand alone unit with secure data therewithin, the computing device being handheld and portable, not necessarily pen-based and if pen-based with no fingerprint sensor in the stylus, the computing device being remote from a host processor and enabling access to network data, the computing device including a pair of fingerprint sensors embedded in the casing, one fingerprint sensor capturing a print image of the user's thumb and the second fingerprint image capturing a print image of the user's index finger, both being of the user's left hand;

FIGURE 3A discloses another preferred embodiment of a computing device for use with the

accessing data and data entry to the data security system of the FIGURE 1;

FIGURES 9A and 9C disclose a simplified logic diagram of one preferred embodiment for requesting access to high security data of the data security system of FIGURE 1, the high security data access request requiring a match authentication of a pair of user fingerprints;

FIGURES 9B and 9C disclose a simplified logic diagram of another preferred embodiment for requesting access to high security data for the data security system of FIGURE 1, the system supplying the user with misinformation if the remote computer is counterfeit;

FIGURE 10A discloses a simplified layout for a user record of one preferred embodiment of the data security system of FIGURE 1;

FIGURE 10B discloses a simplified layout for a data access record for the preferred embodiment of the data security system of FIGURE 10A;

FIGURE 10C discloses a simplified layout for a remote computer record for the preferred embodiment of the data security system of FIGURE 10A;

FIGURE 11 discloses a simplified flowchart for performing a network security audit of the data security system of FIGURE 1;

FIGURE 12A discloses a simplified curve analysis for a regular security environment with the data security system of FIGURE 1, where the threshold position is located at the juncture of the normal curve for authorized users and the normal curve for unauthorized users; and

FIGURE 12B discloses a simplified curve analysis showing for high-security applications with the data security system of FIGURE 1, the curve analysis being similar to FIGURE 12A, where the position of the threshold has been repositioned to minimize false negatives.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to the drawings, FIGURE 1 discloses the preferred embodiment of the data security system of the present invention. The data security system comprises a host processor (12) and a plurality of computing devices (30A, 30B, 30C, 30D). The host computer (12) includes confidential data

that is to be accessed only by authorized users. Some of the computing devices (30C and 30D) are wireless and remote from the host computer (12). The wireless computing devices (30C and 30D) are portable and handheld - and may be pen-based (30C) as shown in FIGURES 1A, 1B, and 1C, or not pen-based (30D) as shown in FIGURES 2A and 2B.

The computing device includes a sensor for capture of a user biometric image - preferably a fingerprint sensor (15). The fingerprint sensor (15) captures an image of a user's finger prior to each request to access data - guarding against unauthorized access to network data (a network security breach). The fingerprint image can also be captured prior to each request to enter new data to prevent contamination of network data.

The capture of the user biometric image is available at continual intervals during routine computer usage. Preferably, the image is captured and compared against a system reference image prior to each request for data access. In another embodiment, the capture occurs continually during predetermined intervals independent of any data access or entry requests. The continual monitoring of user identity provides an added layer of system security.

The capture of the user biometric image is incidental to routine computer usage. The biometric authentication is seamless, as the computer user need only hold the handheld computer is his/her hand similar to holding a conventional handheld computer. The capture of the biometric image is incidental manner to computer operation.

As shown in FIGURE 2A and 2B, at least one fingerprint sensor (15) is positioned at one or more strategic sites such that a portion of the hand of the user is in continuous contact therewith during usage of the processor (30D), enabling a continual authentication of the identity of the user with each request for access to each secure record. The fingerprint authentication is captured in an incidental manner as the data request is submitted from the handheld computer (30D) to the host processor (12) enabling user identity authentication simultaneously with each request to access the secure record. As shown, the processor (30D) includes sensors (15) to capture a thumbprint, the print of the index finger, and a palm print. Also, a palm print sensor (17) can be disposed on the back surface of the computing device (30D) of the present invention to supplement or complement the fingerprint sensors (15). Multiple sensors are recommended for high-security applications (see for example FIGURES 9A and 9B).

FIGURE 3A discloses the frontside of another embodiment of a processor device (20a) for use in another preferred embodiment of the data security system of the present invention. The fingerprint sensor (15) is positioned in the casing (22) of a palm computer (20a), the casing (22) being used to house the palm computer (20a) when used and stored. The casing (22) may also be a wallet or pouch in digital engagement with the processor (20b), either through wire or a wireless mode - enabling identity authentication whenever network access to data is required. The principle advantage of this approach is that registration is conducted through the casing (22) and the computers need not be altered (off the shelf). FIGURE 3B discloses yet another full-screen processor (20b) for use in the data security system of the present invention. These processors (20b) are sometimes referred to as handheld computers in the literature, but are referred to as full-screen processors herein for clarity. The screen is roughly the size of a screen of a PC, except that the computer does not have a conventional keypad. A fingerprint sensor (15) is disposed on one side of the full-screen computer.

FIGURE 4A discloses another preferred embodiment of a computing device (30E) for use in the data security system of the present invention. The handheld computing device (30E) includes a facial image biometric sensor (16) that captures a facial biometric when data access is made from the handheld computing device (30E). FIGURE 4B discloses yet another preferred embodiment of a computing device (30F) for use in the data security system of the present invention. The computing device (30F) is a handheld computer, having a palm image sensor (17) disposed on the backside thereof.

The strategic positioning of individual and multiple sensors depends on the size and shape of the individual computer, and the size of the hands of the computer user. And, it is advised that either the location of the sensors is symmetrical (both sides of the processor) to accommodate both left-handed and right-handed users. Alternatively, some processors can be designed for right-handed users and others for left-handed users.

Referring now to FIGURE 5, the user registers his or her prints by submitting the thumb, index finger, and/or palm prints to the network in a secure process. The reference print is preferably stored in the host processor for security purposes to prevent user access and tampering. The prints may need to be stored in the system also. Subsequently, when network access is requested, the relevant print or prints are captured and compared against